Computer Security Policy

Puddle Ducks regards the integrity of its computer system as central to the success of the organisation. Its policy is to take any measures it considers necessary to ensure that all aspects of the system are fully protected.

Procedure

1. Overall computer security is the responsibility of the data security officer reporting to the managers who are responsible for security within Puddle Ducks.
2. Job applicants will be questioned on their computer experience. The implications of their software knowledge will be discussed with the data security officer before a job offer is made. All references will be checked.
3. On induction employees will be given copies of the computer security policy and will receive written instructions on security procedures.
4. The credentials of all temporary, freelance and consultancy staff should be checked in as much detail as possible before they are allowed access to the computer system. Managers are responsible for ensuring that all such workers receive the information referred to in point 3.
5. Computer training at every level will emphasise the importance of security. Staff will receive a detailed statement on the implications of the Data Protection Act 1998 and the Computer Misuse Act 1990.
6. Supervisors are responsible for ensuring that basic procedures are followed. Procedures may be bypassed only with the combined consent of the line manager and data security officer, and a written record must be kept.
7. Employees of all grades are permitted access only to those parts of the computer system which they need to enter in order to carry out their normal duties. Levels of access will be decided by managers in conjunction with the data security officer who will ensure that levels of access are consistent throughout the organisation.
8.

8. Employees may access the internet but access to certain sites will be blocked.
9. All incoming emails will be monitored and scanned for viruses before being released to the recipient.
10. Employees with access to personal data are in a particularly sensitive position and must bear in mind at all times the provisions of the Data Protection Act.
11. Passwords must be used at all times and changed regularly. Employees should not select obvious passwords. All passwords must be kept confidential. Employees must not give their passwords to other members of staff or to any person outside the organisation. Password protected sites should be closed when finished with and computers switched off. Computers should not be left open and unattended.
12. When an employee leaves the organisation or moves to a different department all passwords in that department will be changed. When an employee is given a temporary password to a higher level of access than he or she normally uses, that password must be cancelled after the individual ceases to need it.
13. Supervisors are responsible for stipulating requirement for back-up operations in their own departments. Regular back up must be carried out in accordance with departmental instructions.
14. All the organisations software must be formally authorised by the data security officer. Regular checks will be made for viruses by the IT department (Jack).
15. No external software may be used without authorisation by both the data security officer and the employee s line manager.
16. No private work or computer game playing is permitted.
17. The safekeeping of CDs and DVDs sent from external sources is the responsibility of the person to whom it was sent. All such CDs and DVDs must be checked for viruses by the IT department before use. CDs and DVDs generated internally must be kept in a secure place.

18 .Misuse of computers is a serious disciplinary offence. The following are examples of misuse:

1. fraud and theft
2. system sabotage
3. introduction of viruses, etc
4. using unauthorised software
5. obtaining unauthorised access
6. using the system for private work or game playing
7. breaches of the Data Protection Act
8. sending abusive, rude or defamatory messages or statements about people or organisations, or posting such messages or statements on any websites or via email
9. attempting to access prohibited sites on the internet
10. hacking
11. breach of the organisations security procedures.

This list is not exhaustive. Depending on the circumstances of each case, misuse of the computer system may be considered gross misconduct. Please refer to the disciplinary rules and procedures. Misuse amounting to criminal conduct may be reported to the police.

19. Management, in consultation with specialist auditors, may institute confidential control techniques and safeguards. Financial systems are subject to special reconciliation processes.

20. Senior managers will meet regularly to review computer security.

21. All breaches of computer security must be referred to the relevant Manager. Where a criminal offence may have been committed, the Managers will decide whether to involve the police.

22. Any member of staff who suspects that a fellow employee (of whatever seniority) is abusing the computer system may speak in confidence to the managers.

This policy does not form part of the contract of employment and any or all of its terms may be amended from time to time.

4.5 In some cases it is not possible for us to specify in advance the periods for which your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria:

(a) the period of retention of personal data category will be determined based on specify criteria .

additional list items

4.5 Notwithstanding the other provisions of this Section , we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

5. Amendments

5.1 We may update this policy from time to time by publishing a new version on our website.

5.2 You should check this page occasionally to ensure you are happy with any changes to this policy.

5.3 We may notify you of changes to this policy by email or through the private messaging system on our website .

6. Your rights

6.1 You may instruct us to provide you with any personal information we hold about you; provision of such information will be subject to:

(a) the payment of a fee

(b) the supply of appropriate evidence of your identity (for this purpose, we will usually accept a photocopy of your passport certified by a solicitor or bank plus an original copy of a utility bill showing your current address) .

6.2 We may withhold personal information that you request to the extent permitted by law.

6.3 You may instruct us at any time not to process your personal information for marketing purposes.

6.4 In practice, you will usually either expressly agree in advance to our use of your personal information for marketing purposes, or we will provide you with an opportunity to opt out of the use of your personal information for marketing purposes.

7. Our details

7.1 This Puddle Ducks is owned and operated by Victoria Stratford and Jacqueline Stratford-Parker .

7.2 We are registered in England and Wales under registration number RP908921 , and our registered office is at address . Abbey farm, Church Lane, Alvingham, Nr LOUTH, Lincolnshire, LN11 0QD

7.3 As above

7.4 You can contact us:

(a) by post, to the postal address given above ;

(b) using our website contact form ; puddleduckspreschoolalvingham.co.uk

(c) by telephone, on the contact number published on our website from time to time ; or

(d) by email, using the email address published on our website from time to time .

face to face, through Baby days or Tapestry (on line learning journey)

8. Data protection officer Jacqueline Stratford-Parker

8.1 Our data protection officer's contact details are: Puddle Ducks, Abbey Farm, Church Lane, Alvingham, Nr LOUTH, Lincolnshire, LN11 0QD .